法 学 研 究

何谓数据主权?
——全球数字规则博弈中的弹性主权视角

刘　晗

(清华大学 法学院, 北京 100084)

摘　要: 在当前全球数字秩序经历深刻变革的背景下,“数据主权”逐渐成为各国重申其国家数字控制力、应对平台治理失衡现象以及规范数据跨境流动的关键话语工具。数据主权不应被简单视为传统主权在数字领域中的直接映射,而是一种具有高度灵活性,同时具备进攻和防御双重结构的弹性主权形式。在理论上,需要区分两种类型的数据主权:“消极数据主权”(体现为数据本地化、防御措施及地域控制)与“积极数据主权”(表现为规则外溢、平台嵌入及架构控制)。两种数据主权在全球数据治理进程中的交互演变,形成了国家、数字平台与跨国法律结构间的新型主权张力。就全球数字治理而言,应以超越传统领土主权的新型主权理论为依托,重构全球数据治理秩序及其正当性基础。

关键词: 数据主权;跨境数据流动;积极主权;消极主权;全球治理

中图分类号:D911.01　　**文献标识码:**A　　**文章编号:**1000-5919(2025)06-0115-12

在大数据、云计算和人工智能飞速发展的推动下,数据迅速成为兼具商业、社会与战略价值的关键资源,甚至被誉为新技术时代的“石油”,成为国际政治经济战略竞争中的重要变量。在贸易与安全的双重角力下,众多国家纷纷将网络主权的关注焦点延伸至数据领域,“数据主权”由此成为数字时代的重要国际话语之一。① 然而,学界关于数据主权的概念迄今尚未达成共识。主流观点将数据主权界定为国家主权在数据领域的应用,即国家对本国境内产生的数据进行管理与利用的权力,②域内表现为国家对数据及相关技术、设备等的管辖权,域外表现为与数据相关的国际事务合作权和参与权。③ 另有观点认为,数据主权主体不仅包含国家,还应包括企业和个人,④公司尤其是事实上的数据主权者。⑤ 也有论者将数据主权权属区分为国家对本国数据的管理权、企业通过提供服务换取的用户数据永久使用权和用户个人的信息隐私权。⑥ 种种分歧表明,数据主权概念,既是认知的基本起点,也是语义争夺的场域。本文旨在厘清数据主权的生成逻辑及其内涵外延,试图超越将传统国家主权套用于数据问题的常见逻辑,转而从数字时代主权的弹性结构出发,重新理解其内在张力。本文提出,数据主权分为“消

收稿日期:2025-03-27

作者简介:刘晗,清华大学法学院长聘教授。

基金项目:北京市社会科学基金青年学术带头人项目“比较视野下中国宪法实施体系的演进、模式与未来”(24DTR047)。

① Patrik Hummel et al., *Data Sovereignty: A Review*, Big Data & Society, Vol. 8(1), 2021, pp. 1-17.

② 参见曹磊:《网络空间的数据权研究》,《国际观察》2013 年第 1 期,第 53—58 页。

③ 参见孙南翔、张晓君:《论数据主权——基于虚拟空间博弈与合作的考察》,《太平洋学报》2015 年第 2 期,第 64—65 页;齐爱民、祝高峰:《论国家数据主权制度的确立与完善》,《苏州大学学报(哲学社会科学版)》2016 年第 1 期,第 83—88 页。

④ 参见杜雁芸:《大数据时代国家数据主权问题研究》,《国际观察》2016 年第 3 期,第 1—14 页。

⑤ 参见翟志勇:《数据主权时代的治理新秩序》,《读书》2021 年第 6 期,第 96—97 页。

⑥ 参见冯伟、梅越:《大数据时代,数据主权主沉浮》,《信息安全与通信保密》2016 年第 6 期,第 49—51 页。

极数据主权”与“积极数据主权”两种类型,前者强调数据本地化、防御机制与地域控制,后者则聚焦规则外溢、平台嵌入与架构塑造;在此基础上,指出两者在全球数据治理中交互演化,构成国家、平台与跨国法律结构之间的新型主权张力。回应当前数字主权的理论难题,需要以超越领土中心的弹性主权观为基础,重构全球数据治理的秩序与正当性逻辑。

一、数据主权问题的缘起与现实体现

虽然“数据主权”一词近年来才广泛流行,但其核心关切早已存在于互联网发展过程中。国家对于数据安全、信息控制与技术规范的主权诉求,早在 20 世纪 90 年代便不断显现。从物理层的网络基础设施控制,到逻辑层的协议标准主导,再到内容层的言论治理与数据流动规制,国家从未曾缺席。

(一)长期存在的推动因素

数据主权是网络主权的概念延伸。曾经促使主权在网络空间内不断发展的诸种因素,也构成了数据主权兴起的底层因素。

首先,信息和数据跨境流动自互联网初步普及的 20 世纪 90 年代即存在。彼时,互联网的无疆界特性导致信息传输超越国界,由此产生管辖权争议,促使各国开始酝酿控制信息流通的法律与政策。① 只不过,当时很多国家禁止违反本国法的信息流入。② 而今日,很多国家则限制本土产生的数据外流。③ 这既展现了从网络主权到数据主权的延续,也凸显了断裂。

其次,安全始终是互联网发展的核心要素。从最早防范计算机病毒,到防止黑客攻击,再到“9·11”事件后各国加强信息基础设施防护,网络与数据安全的重要性持续上升。过去十余年间,以国家安全为导向的数据管控与情报搜集,使各国愈发意识到数据治理的必要性。2013 年斯诺登曝光“棱镜计划”后,各国加快构建网络安全的技术与法律体系,并推动“数据主权”概念显现。可以说,数据主权正是网络安全上升为国家安全的集中体现。

最后,个人信息和隐私权的保护早已成为重要议题。早在 20 世纪 80 年代,德国联邦宪法法院便确立了“信息自决权”。近年来,隐私保护日益成为推动数据主权与本地化的重要动力。各国逐渐意识到,唯有将公民数据储存在本国,并纳入本国法律严格监管,方能有效防范外国机构的侵犯。数据本地化法律的兴起,既是国家履行保护职责的体现,也为强化数据主权提供了法律支撑。

(二)近年来的新推动因素

大数据与云计算技术的兴起极大地挑战了传统数据治理模式,促使数据主权概念获得新的内涵,也使数据主权问题日趋紧迫。

首先,云计算打破了数据存储的物理属地性质。“云计算是一种利用互联网实现随时随地、按需、便捷地访问共享资源池(如计算设施、存储设备、应用程序等)的计算模式。”④这种模式将数据从本地移到云端,体现为“联网设备显示存储在远程服务器而非设备本身数据的能力”⑤。于是,“数据作为一种新的生产要素,具有开放性、跨时空和共享特征”⑥。正如文件共享技术挑战版权法,比特币挑战货币发行权,云计算则挑战了法律管辖权,造就了数据的非领土性特征。⑦ 数据无处存在,又无处不在。

---

① See David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, Stanford Law Review, Vol. 48(5), 1996, pp. 1367-1402.

② 参见政武:《巴黎法院对“雅虎案”裁定的法律思考》,《互联网生活》2001 年第 2 期,第 81—82 页。

③ See Anupam Chander & Uyê P. Lê, *Data Nationalism*, Emory Law Journal, Vol. 64(3), 2015, p. 679.

④ 罗军舟、金嘉晖、宋爱波等:《云计算:体系架构与关键技术》,《通信学报》2011 年第 7 期,第 4 页。

⑤ *Riley v. California*, 573 U.S. 373, 397(2014).

⑥ 周文、叶蕾:《新质生产力与数字经济》,《浙江工商大学学报》2024 年第 2 期,第 20 页。

⑦ See Jennifer Daskal, *The Un-Territoriality of Data*, Yale Law Journal, Vol. 125(2), 2015, pp. 326-399.

其次,数字经济和人工智能的兴起使数据成为关键战略资源。数据不再仅是隐私或安全问题,更是国际经济竞争和战略博弈的焦点。近年来,美国针对 TikTok 和华为的禁令、印度对中国应用软件的封禁措施、欧盟针对美国提出"数字主权"等主张,均将数据问题明确地与地缘政治、国家安全和数字战略捆绑在一起。

最后,云计算技术的广泛应用改变了全球信息领域的地缘政治格局,强化了国家间的不对称关系。这不仅体现在发达国家与发展中国家之间,甚至也存在于发达国家之间。例如,西方世界超过九成的数据存储集中于美国的云基础设施。① 美国也通过国内法律制度对全球范围内的数据流动实施控制。即便欧洲用户的数据存在本地,仍可能被美国平台与政府跨境访问。

(三)数据主权问题引发的法律讼争

在上述背景下,关于数据跨境的法律讼争也日益普遍。当一国企业掌握的数据存储在他国并受该国法律约束,而母国公权力机关试图调取这些数据时,数据主权问题便会浮现。如果外国执法机构频繁使用"长臂管辖",冲突则会进一步加剧。

一个典型案例是"微软案",该案集中展现了数据跨境与国家主权之间的冲突。② 美国联邦调查局(FBI)曾要求微软提供其存储在爱尔兰数据中心的用户邮件内容,以协助调查一起毒品案件。FBI 认为,尽管数据位于境外,微软作为美国公司对其拥有控制权,理应配合调查。微软拒绝配合,主张强制调取可能违反爱尔兰法律及欧盟数据保护规则,侵犯了爱尔兰的"数据主权"。美国联邦第二巡回法院初审支持微软,认为 FBI 应通过司法互助程序请求爱尔兰授权,而非直接越境执法。然而案件上诉期间,美国国会通过《云法案》(CLOUD Act),授权执法机关可要求美国公司提供其"掌握"的数据,无论数据存于何地。法案通过后,美国最高法院认定原案"已无审判意义"(moot),随即撤销下级法院判决,变相承认了美国政府对境外数据的强制获取权。在诉讼过程中,爱尔兰政府亦提交意见,指出美国执法机构不仅违反爱尔兰隐私法,亦违反欧盟《数据保护指令》(DPD)。尽管这些主张曾被美国的下级法院采纳,最终却被新法排斥。

这一事件成为"数据主权"与"跨境执法"冲突的典型案例,标志着围绕数据的国际法律冲突由政策博弈升级为制度碰撞。这种碰撞突破了传统领土边界,转向"谁有权制定并强制执行数据规则"的根本问题。在更大的意义上,数字技术的运用塑造的新兴业态和国际贸易模式,也使传统国际经贸规则亟须重塑。③ 因此,"数据主权"并非政治口号,而是国家主权在全球信息流动和数字经济格局中重新塑形的集中体现。它揭示的是法律原则、国际秩序与技术现实之间的结构性张力。我们亟须回到主权概念本身,审视其在数字时代的变迁,以理解数据主权的真正含义。

二、数据主权的内涵:超越领土边界的权威与控制

就概念起源而言,主权是指一个政治体内的最高权力,不受内外其他组织或力量的挑战。④ 主权的定义蕴含着权威性、领土性和排他性三个要素。数据流动性对上述三个要素构成了挑战:其一,权威构建从传统模式日益转向依赖实际控制;其二,主权边界在数字化浪潮下被重新塑造;其三,在私营平台环境中,主权博弈局面日益复杂。

---

① See Synergy Research Group, *Hyperscale Cloud Market Grows Strongly in* 2023, www. tietoevrytechservices. com/siteassets/03-files/whitepapers/tech-services-digital-sovereignty-whitepaper-v1-2023. pdf, pp. 5-6.

② See *United States v. Microsoft Corp.*, 584 U. S. 236(2018).

③ 参见沈坤荣、李敏:《国际经贸规则重塑背景下中国推进制度型开放的战略思考》,《浙江工商大学学报》2023 年第 6 期,第 82 页。

④ See Jean Bodin, *The Six Bookes of a Commonweale*, Richard Knolles trans., Impensis G. Bishop, 1606, p. 84.

(一)权威性:法律权威与实际控制的复杂关系

主权不仅是一种法律权威的宣示,更是一种实际控制的权力。前者是指国家从事各种活动的合法权利和正当资格;后者则是指通过硬实力和软实力所实现的有效管理。① 数据主权同样可以从这两个维度加以理解。国家有权管控数据跨境流动,这一原则已逐渐成为国际共识。更具挑战性的是对数据流动的实际控制能力,包括数据保护的技术能力和数据的互操作性能力(即在跨境环境中交换与使用数据的能力)。数据主权不仅是宣称“应当能管”,更关乎“是否真能管”。

主权的深层逻辑在于,实际控制程度会影响法律权威。一国对数据流动的掌控力取决于其政治、经济和技术等综合实力。“技术的落后和依赖性转化为安全和经济机会的减少,最终是主权的丧失。”② 在常见的数据主权界定中,无论是管辖权、防卫权还是独立权,都旨在防御他国通过新兴技术推行霸权主义,如透过网络空间干涉别国内政,或者凭借技术优势损害别国基础设施和通信体系等。很多国家主张对于数据拥有管辖权,但由于技术能力和国际压力等因素难以实现实际控制。它们提出数据主权,是因为意识到:失去对于数据的实际控制,有可能丧失管治权威。

反过来,网络强国可能会将控制扩展到正式权威之外。网络强国利用自身在数据采集、处理、控制与调取上的优势,让网络弱国不仅难以保护本国公民信息,也无法保障国家独立安全,引发“数据殖民主义”的担忧。③ 当代很多发展中国家提出“数据主权”,就带有此种色彩。网络强国也可以对“数据主权”保持沉默,甚至在尊重他国主权的修辞之外,通过对数据的实际控制来实现自身的主权扩张,从而加剧数字时代的主权错位。

(二)领土性:越过国界的主权边界

主权的空间形态始终与技术发展紧密相连。没有技术,权威就无法投射为实际控制。回顾历史,每次重大技术突破都催生新的主权疆域:造船术与航海术打开了海洋;航空技术造就了“领空”;人造卫星与航天器引发了“外层空间”归属之争;互联网技术让“网络空间”成为主权的新前沿。大数据与云计算技术的普及,让虚拟的数据成为主权争夺的新领域。④

现代国家之间相对精确的领土边界,得益于测绘与制图技术的发展。历史上,国家并非始终依据明确边界线彼此划分:中国古代多以“城池”为界,早期现代欧洲国家间则常存在模糊的“边疆”,而非清晰的“边界”。⑤ 精确界线的划定最初源于现代欧洲,随后扩展至全球。⑥

进入大数据与云计算时代,国家对数据的控制正催生新的“地图绘制术”。“边境”不再是物理的国界或口岸,而是虚拟的网络连接点。数据主权的边界呈现出多重交织、动态流变的形态,难以如界碑或围墙般清晰标示。判断标准趋向“实质重于形式”,需综合考量数据接收方的国籍、所在地、设备位置、数据存储地、处理实体的法律归属、员工国籍,以及数据是否可被境外访问及其权限范围等因素。⑦ 例

---

① See Stephen Krasner, *Sovereignty: Organized Hypocrisy*, Princeton University Press, 1999, p. 10.

② *Presidential Address to the Federal Assembly*, http://en.kremlin.ru/events/president/news/56957.

③ See Nick Couldry & Ulises A. Mejias, *Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject*, Television & New Media, Vol. 20(4), 2019, p. 337.

④ See Roxana Vatanparast, *Data Governance and the Elasticity of Sovereignty*, Brooklyn Journal of International Law, Vol. 46(1), 2020, p. 35.

⑤ See Lucien P. V. Febvere, *Frontiere: The Word and the Concept*, in Peter Burke ed., *A New Kind of History: From the Writings of Febvere*, K. Folca trans., Harper & Row, 1973, pp. 208-218.

⑥ See Michael Biggs, *Putting the State on the Map: Cartography, Territory, and European State Formation*, Comparative Studies in Society and History, Vol. 41(2), 1999, pp. 374-405.

⑦ 参见戴翔:《“边界”在何处——数据跨境传输之辩》, https://www.dehenglaw.com/CN/tansuocontent/0008/022852/7.aspx? MID=0902。

如,即便数据存于云端,其在特定国家数据中心的落点仍可能受该国法律约束。再如,数据可借虚拟网络穿越多个司法辖区,关键在于识别数据何时、如何进入不同的监管环境。因此,数据跨境的界定已不再取决于单一物理位置,而是涵盖存储位置、传输路径与处理行为等复合维度。国境不再局限于地理疆界,而是由国家实质利益需求与实际控制能力共同界定的动态边界。这一边界灵活多变,随着国家战略目标与技术掌控能力的变化而不断被调整。

上述特点已经体现在相关法律法规中。如我国《数据出境安全评估申报指南》规定,数据出境不仅指数据被直接传输至境外,还包括“数据处理者收集和产生的数据存储在境内,境外的机构、组织或者个人可以查询、调取、下载、导出”①等情形。再如,欧盟 GDPR 中的“边界”也是由数据主体(即欧盟公民)的所在地和数据处理活动的位置来定义。② 美国《加州消费者隐私法》(CCPA)也根据与加州居民的相关性定义数据边界,至于数据处理者位于何处则在所不问。③

(三)排他性:数据主权蕴含的三角结构

在传统语境下,主权的排他性体现为一国在其领土内排除其他国家的干预。然而,数字时代私营超级平台的崛起打破了这一格局。全球数据主权博弈已由国家间对峙演变为“国家 A—平台—国家 B”的三元结构。平台一方面受多重主权的法律约束,另一方面又凭借技术优势深度介入国家间的数据控制博弈。它成为制度性中介,重塑主权的实现路径与合法性结构。在这一结构中,B 国的数据、市场、舆论与基础设施可能被 A 国的平台深度渗透,而 B 国却难以实施有效监管:要么因平台不完全受其属地法约束,要么因管制行为可能招致 A 国反制。平台既是管道,也是权力再分配者,挑战了传统主权的执行逻辑。

随着数字经济不断发展,特别是当平台利用数据优势实现市场支配地位甚至滥用此地位时,④平台的中立性神话已被打破。在跨国数据平台深度介入信息收集、数据处理、内容分发与身份识别等治理活动之后,平台已成为事实上的治理者。平台通过“服务条款”“社区准则”“算法排序”形成对用户行为的实质规范,并对信息可见性、表达自由乃至集体行动能力施加影响。⑤ 因此,平台企业凭借数据垄断、算法设计和网络治理三重优势,实质上扮演着比喻意义上的“数据主权者”角色。⑥

平台之为“数据主权者”,体现在两方面:一是平台嵌入国家治理,挑战国家在信息与身份管理上的垄断,其治理体系虽非国家法所生,却具备类宪法功能(制定规则、设限权力、回应合法性诉求),并与国家宪制结构交织互动;二是平台背后的国家凭借其技术与治理优势,对外输出影响力,使平台成为国家战略延伸的工具。超级平台虽无公权徽章,却通过掌控数据和代码规则重塑信息权力的配置范式。

在前述三元结构中,常常出现三重博弈关系。其一,平台挑战本国主权。如 2019 年脸书计划推出数字货币 Libra,意在绕开现有国家银行系统,动摇货币主权,引发美国国会强烈反弹。扎克伯格甚至说:“脸书更像是一个政府,而不是一家传统公司。”⑦其二,平台挑战他国主权。若外国科技企业在东道国收集数据、输出影响,而该国缺乏监管能力,便可能形成数据层面的“间接殖民”。其三,平台成为

---

① 《数据出境安全评估》(2025)一(二)2。

② See Regulation (EU) 2016/679(General Data Protection Regulation), Art. 3(2). 后文引用该条例时,简写为 GDPR。

③ See California Civil Code, § § 1798.100-1798.199(California Consumer Privacy Act of 2018).

④ 参见朱志峰、夏迪旸:《超级平台利用数据优势滥用市场支配地位行为的监管完善》,《商业经济与管理》2023 年第 10 期,第 91 页。

⑤ See Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, U.C. Davis Law Review, Vol. 51(3), 2018, pp. 1149-1210.

⑥ 胡凌:《探寻网络法的政治经济起源》,上海:上海财经大学出版社 2016 年版,第 34—39 页。

⑦ Ezra Klein, *Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next*, Vox, April 2, 2018.

国家间数据争夺的工具。主权争夺常通过平台的技术标准、服务器布局与数据访问权的博弈展开。微软案即体现了平台在跨国数据调取中的关键角色。

跨国数字平台的“国籍”已成为数据主权博弈的核心议题。关键不在于注册地,而在于实际控制权归属。这一判断涉及 VIE 架构、运营重心与控制链等复杂因素,既模糊又敏感,成为引发国际冲突的高风险点。2020 年以来,TikTok 与美国政府的对峙即为典型。尽管 TikTok 强调本土注册、设立美国数据中心并强化合规,且其母公司注册于开曼群岛,美国仍以“国家安全”为由施压,要求其剥离在美业务。① 可见,数字平台的“国籍”认定,越来越取决于地缘政治判断,而非法律或商业形式。

数据主权冲突已不再局限于传统公法领域,私法诉讼正成为国家主权行使的重要方式。表面上,这类案件涉及隐私权、消费者权益或合同纠纷,实则反映国家对平台行为的主权介入。“谷歌西班牙案”最为典型:虽系个人要求删除搜索结果链接的隐私诉求,实质上是欧盟法院对美国平台施加法律约束的主权宣示,裁定其欧洲子公司应受欧盟法规范。② 再如,韩国 2021 年修订《电信事业法》,禁止应用商店强制内建支付系统,被称为“反谷歌法”,表面是保护开发者和消费者权益,实则意在规制跨国平台的市场支配力。③ 在此类情境中,数据主权不再仅体现为国家安全或数据本地化,而是通过调整商业规则、支付路径与数据流向,将主权控制嵌入私法机制与市场秩序,实现对平台的有效治理。

三、数据主权的外延:扩张性主权与防卫性主权

主权观念涵盖积极扩张和消极防御两个维度。通常情况下,主权多从消极层面被理解,与保护国家免受外部侵犯的防御举措相关联。但当认识到实际控制能力能向法律权威转化时,主权的积极扩张性就显现出来。此前,这一面向一直较为隐匿;如今,数字化将其充分激发。

(一)主权的伸缩性:积极与消极

以赛亚·柏林曾区分消极自由(不受干预)和积极自由(自我主宰)。④ 这一区分同样可用于理解国家主权的双重面向:消极主权和积极主权。⑤ 消极主权强调排他性、自主性与边界控制,防止外部干预;积极主权则意在塑造认同、输出治理、争夺规则主导权。传统的威斯特伐利亚体系主要体现消极主权:各国承认彼此领土与政治独立,互不干涉。但积极主权从未缺席:16 世纪至 19 世纪,欧洲列强在本土遵守边界规则,却在海外进行殖民扩张;19 世纪末至 20 世纪,各类帝国主义追求的不是平等主权(sovereignty),而是凌驾其上的世界主权(imperium)——无论是“大英帝国”“第三帝国”“苏维埃帝国”,还是“美利坚帝国”。

美国是“积极主权”的典型代表。其全球扩张并不依赖传统的占领与殖民,而是借助贸易、金融与法律规则穿透边界,攫取实质控制权。在法律上,美国以国际经济法取代传统国际公法,通过制度设计实现对他国的间接支配,避免触犯形式主权,却施加深度影响。即便是高调主张“美国优先”的特朗普,也延续了这一扩张逻辑,只不过更加赤裸:无论是扬言吞并加拿大、购买格陵兰,还是以关税手段对全球施压,皆体现了美国将主权作为对外施力工具的积极用法。⑥

---

① *TikTok, Inc. v. Garland*, 604 U.S.(2025).

② See Case C-131/12, *Google Spain SL v Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, May 14, 2014.

③ See Act. No. 2112203, Aug. 31, 2021(South Korea); Yunsieg P. Kim, *Does the Anti-Google Law Actually Help Google and Hurt Startups?* Georgetown Law Journal Online, Vol. 110, 2021, pp. 120-134.

④ 参见以赛亚·柏林:《自由论》,胡传胜译,北京:译林出版社 2003 年版,第 189 页。

⑤ See Paul W. Kahn, *The Question of Sovereignty*, Stanford Journal of International Law, Vol. 40(2), 2004, p. 260.

⑥ 参见章永乐:《“主权主义者”特朗普?》,《广角镜》2025 年第 3 期,第 30 页。

总而言之,主权其实一直在跨越领土边界,对人员、物品和事务实施有效控制并施加影响。①“主权不是固定的一个法律外衣,而是内化为多层次、要素、色彩与光谱的复合体,具有明显的伸缩性与延展性。”②

(二)弹性数据主权:积极与消极

数字时代,主权呈现出封闭与开放并存的特征:既突破疆界,又重塑管辖逻辑;既被动守边,又主动造界。数据主权的核心问题,在于法律如何构建主权的弹性,以及这种弹性如何在权力分配与相互授权中体现出来。实践中,数据主权的边界多由国家利益所界定,而非固定规则。在全球治理博弈中,主权弹性主要体现为两种理想型路径:一是消极路径,侧重防御、本地化与数据外流管控;二是积极路径,借助技术、平台与规范输出,推动跨境整合与规则制定,展现国家对数字秩序的主动塑造能力。

1. 消极数据主权:以本地化为中心

消极数据主权是传统威斯特伐利亚主权在数字时代的延伸,侧重防止境外主体擅自获取、分析与利用本国数据,以维护国家安全与公民权益。它既针对外国政府的数字干预,也防范跨国平台对本国数据的控制。主要措施包括数据本地化、跨境传输审批以及对外资平台的数据处理义务设定。按规范强度不同,可区分为强弱两类。

强版本下,国家对数据跨境流动设定严格限制,通常要求在本国采集的个人数据必须在境内存储和处理,未经批准不得传输至境外。中国《网络安全法》《数据安全法》《个人信息保护法》要求对重要数据和个人信息的跨境传输须进行安全评估、签署标准合同或通过认证。③ 印度《数字个人数据保护法》对敏感个人数据和关键数据的跨境传输设定限制,要求此类数据必须在印度境内存储和处理,除非满足特定条件。④ 越南《网络安全法》《个人数据保护法令》也有类似规定。⑤

弱版本下,国家允许数据在满足特定条件下跨境流动,通常要求接收国具备足够的数据保护水平,或者通过合同等法律工具保障数据安全。如欧盟 GDPR 允许特定条件下的数据跨境传输,如接收国被认定为能够提供充分的数据保护,或者通过标准合同条款等机制。⑥ 南非《个人信息保护法》允许在特定条件下进行个人信息的跨境传输,如接收方所在国家具有类似的数据保护法律,或者数据主体明确同意。⑦

值得注意的是,当前的数据本地化立法,已不再仅以技术手段锁定数据于本国境内,而是逐步发展出域外管辖机制:即便数据处理活动发生在海外,只要涉及本国公民或本国组织的数据,就必须遵守本国法律。欧盟 GDPR 明确规定:“本条例适用于不在欧盟设立机构的数据控制者或处理者,只要其处理涉及位于欧盟境内的数据主体的个人数据。”⑧中国《数据安全法》第二条规定,该法不仅适用于中国境内开展数据处理活动的主体,也包括对中国境内的自然人或组织的权益产生影响的境外数据处理活动。

---

① See Roxana Vatanparast, *Data Governance and the Elasticity of Sovereignty*, p. 5.

② 王逸舟:《当代国际关系的进步:若干线索》,载微信公众号“政治学与国际关系论坛”,2022 年 7 月 6 日。

③ 参见《中华人民共和国网络安全法》第 37 条;《中华人民共和国数据安全法》第 31 条;《中华人民共和国个人信息保护法》第 38—40 条。

④ See Digital Personal Data Protection Act, No. 22 of 2023, § § 15-17(India).

⑤ 参见王勤:《越南数字经济的转型战略和发展前景》,《广西社会科学》2025 年第 3 期,第 65 页。

⑥ See GDPR, Arts. 45-46.

⑦ See Protection of Personal Information Act, No. 4 of 2013, § 72(South Africa).

⑧ GDPR, Art. 3(2).

巴西、土耳其和尼日利亚等国的法律都有类似规定。① 由此可见,很多国家已经通过属人、属地和"属效果"的三重管辖设定,将数据主权的保护边界推展至境外。这一趋势表明,即使是以防卫为核心的消极数据主权,也具有主动设界并向外辐射的能力。

2. 积极数据主权:以扩张与规则输出为核心

积极数据主权表现为外向型主权逻辑:国家通过控制全球信息架构、平台规则与法律外溢手段,对他国数据活动进行间接或实质控制。其核心不是防卫性和排他性,而是数据流动控制力和数据规则输出权,试图实现国家在全球数字治理体系中的战略主导。这种主权并不依赖于领土控制,而是通过架构内嵌和标准设定来实现。

在架构内嵌语境中,国家通过本国控制的信息基础设施,将自身的价值观、法律规范和科技伦理嵌入全球数据流通和数字经济之中,形成隐性主权输出。谁控制了数据的流通管道,谁就能将主权主张嵌入其中。例如互联网的"根"控制权:美国控制着大多数根域名服务器,并且通过 ICANN 等控制 IP 地址分配,使得全球大部分网络运行须依赖由美方主导的基础机构,从而接受其政策设定。再如云平台支配力:亚马逊、微软和谷歌提供的云服务主导全球市场,可以在云服务中设定数据处理和隐私规则,使境外客户也可能受美国法约束。再如软件生态嵌入:美国通过操作系统、浏览器、广告协议等应用在全球的大范围部署,使得全球用户在使用美国前端应用时,就已默认遵奉其后端监管逻辑。再如全球数据汲取力:《云法案》赋予美国执法机构跨境调取由本国企业控制的数据的权力,无论数据存储于何地,只要企业受美国司法管辖,即可实质获取。于是,美国通过数字技术实现对他国新型控制,实施信息监控与资源攫取。科技巨头依托平台生态深度嵌入他国政治、经济与文化体系,稳固美国在全球数字秩序中的主导地位。②

在标准设定语境中,一个国家或政治体通过将本国法律、价值观与政策偏好"外溢"为国际规则,塑造他国政府与企业的行为选择。谁能率先设定并推广标准,谁就有可能主导正在成型的全球数据治理体系。例如,欧盟虽非网络强权,却堪称网络规制强权。GDPR 通过"域外适用""合规认证"等制度设计,将其数字人权理念和人格尊严法理嵌入国际规范框架,形成所谓"布鲁塞尔效应"。③ 这不仅依赖于欧盟法律制度的技术精致性,还依靠其在话语塑造、经济影响与制度示范等方面的综合实力。一是规则输出:GDPR 被视为全球"金标准",引发包括日本、巴西、韩国、肯尼亚等多国仿效其立法模式。二是跨境数据治理:欧盟通过充分性标准机制,对外评估哪些国家的数据保护水平足以接受欧盟个人数据流入,从而设定进入全球数据流通体系的合规门槛。三是数字市场监管:欧盟相继推出《数字市场法案》与《数字服务法案》,不仅作为内部市场规制工具,更借此向全球跨国平台施加合规义务,扩展其规制权力边界。④

3. 两种主权的交错表现与动态张力

积极主权和消极主权的区分并非与特定国家政策的机械对应,而应视为韦伯意义上的"理想类型"。两者在现实中并非泾渭分明,而是交错存在。国家可能同时展现出两者,并在历史演进和现实格局中不断交错变换。

---

① Lei No. 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais, Art. 3 (Brazil); Law on the Protection of Personal Data, No. 6698, Art. 9, 2016 (Turkey); Nigeria Data Protection Act, No. 4 of 2023, § 41 (Nigeria).

② See Michael Kwet, *Digital Colonialism: US Empire and the New Imperialism in the Global South*, Race & Class, Vol. 60 (1), 2019, pp. 3-26.

③ See Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

④ See GDPR, Arts. 45-46; Regulation (EU) 2022/1925 (Digital Markets Act); Regulation (EU) 2022/2065 (Digital Services Act).

以美国为例。它一方面倡导全球数据自由流动,以利其科技平台主导全球市场;另一方面,在面临潜在竞争者时,又迅速展现消极主权一面,强调国家安全和数据本地化。两者都旨在维护美国的数字主导地位。尽管时常宣称互联网自由,美国始终未放弃对网络空间的主权控制。施米特在论述现代早期全球秩序时说:“坚固的陆地从属于一群主权国家,而海洋则不属于任何国家,或者说属于所有的国家……实际上最终只属于一个国家:英国。”①美国互联网自由论的实际含义是,互联网不属于任何国家或属于所有国家,实际上只属于一个国家:美国。在一段时期内,美国在否认主权存在于网络空间的同时,将自己视为网络空间中的唯一主权者。

在数据治理领域,美国法律政策始终以市场自由与技术优势最大化为导向,奉行数据外流为常态、流动管制为例外的基本原则,体现出结构性进攻与个案式防御相结合的战略逻辑。在国内,美国并无联邦层面的数据本地化立法,原则上不禁止企业跨境传输美国公民数据,仅针对特定敏感数据向特定国家的传输设立明确禁令和限制;②在国外,则积极推动数字贸易协定,反对本地化,倡导跨境数据自由流动。③ 唯一的例外发生于国家安全层面。在 TikTok、华为等案例中,美国以国家安全为由,对涉及美国公民数据的外国背景的公司进行审查。总体而言,美式数据主权以攻为主、攻守兼备。只是随着他国科技实力提升,其防御面的存在感才日益凸显。

美式数据自由流动的背后,是一套明确的双轨逻辑:对外,数据流动不得危及国家安全;对内,数据获取服务于全球战略。1978 年《外国情报监控法》授权政府监控境外目标,2001 年《爱国者法案》将监控范围扩大至本国公民,2018 年《云法案》则突破国籍与地域限制,允许全球调取数据。同时,美国通过外国投资委员会机制(CFIUS)将国家安全审查延伸至数据领域,凡在美有实质运营的企业,均受其法律约束,无论其所有权结构如何。20 世纪初,美国战略是“经济在场,政治缺席”; ④而在 21 世纪,《云法案》体现的是“法律在场,政治隐身”的模式。借助科技平台的全球布局,美国实现了企业所至、主权随行的治理模式。反观他国,若欲调取美国或其境内他国公民的数据,须先被认定为“合格外国政府”,即达到美方标准,实质上排除了真正的对等待遇。⑤

美国对全球数据的事实垄断,引发多国高涨的数据主权诉求。面对美国超越国界的控制力,各国推动的数据本地化立法,是“边缘”对“中心”的结构性抵抗。这类立法并非单纯的地方保护主义,而是因未参与规则制定,也缺乏改变格局的制度通道,却长期承受数字剥削与信息支配所引发的主权回应。这是一种政治表达,更是对数据霸权的制度性拒斥:“你在你的疆域主导秩序,我在我的疆域守住底线。”

由此可见,主权的弹性不仅体现在疆域逻辑上的伸缩,更体现于主权姿态的灵活切换。在全球数字治理趋于碎片化的今天,数据主权的双重形态揭示了主权从物理向信息、从地理向网络、从边界向节点的深层转变。这种攻守并存、攻防转换的结构逻辑,将成为未来国际秩序重塑中不可忽视的张力。

四、数据主权的意涵:全球数据治理中的制度争衡

厘清数据主权的内涵与外延后,分析重心需要转向全球数据治理的制度格局。当下,各国围绕规则制定、标准设定与平台管辖激烈博弈,全球格局呈现出类似“战国”的多边竞争态势。同时,治理也展现出“有限共生”的特征:国家在坚持主权边界的同时,亦在跨国规则中争取话语权与协商空间。

---

① 卡尔·施米特:《陆地与海洋:世界史的考察》,林国基译,上海:上海三联书店 2018 年版,第 54 页。

② See US Department of Justice, Preventing Access to U. S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (implementing E. O. 14117), 2024-31486 (90 FR 1636).

③ United States-Mexico-Canada Agreement, July 1, 2020, Ch. 19.

④ 参见卡尔·施米特:《大地的法》,刘毅、张陈果译,上海:上海人民出版社 2017 年版,第 276 页。

⑤ 参见洪延青:《美国快速通过云法案,清晰明确数据主权战略》,《中国信息安全》2018 年第 4 期,第 54—56 页。

(一)全球数据治理的碎片化格局

当前全球互联网治理已经走出“互联网自由论”的单一叙事,逐步进入多元主权理念并存、规则体系互不兼容、网络空间主权化的割据时代。正如战国时期各诸侯国制礼作乐、度量不同,今日世界的数据主权格局呈现出诸种模式并存的竞争格局。

一是美国模式。它强调“数据自由流动”与平台驱动的全球市场逻辑,以私营平台为抓手构建国际秩序。美国在法律上以宪法第一修正案中的言论自由原则为基础,在政策上主张最小化国家干预,通过推动私营科技企业建立合规机制维系治理框架。其战略核心是维持自身对全球技术底座和数据分发网络的结构性主导权。

二是欧盟模式。它主张以数据权利保护为中心,通过法律法规体系建立起全面的数据治理标准。欧盟强调数据处理中的知情同意、数据可携带权与删除权,并通过“充分性认定”将欧盟数据主张向外延伸,体现出规范性制度外溢的逻辑。欧盟模式构建起一种“权利本位型数据主权”,强化对个人信息的制度保障,也推动企业形成更高合规标准与治理透明度。

三是中国模式。中国通过《数据安全法》《个人信息保护法》等系列立法,构建起以国家安全为重要原则的数据治理体系。中国还在“一带一路”倡议框架下,通过“数字丝绸之路”推动海外数据中心、云服务设施与海底光缆建设,试图降低全球对西方主导的数字基础设施的依赖,打造新的数据流通网络。上述法律和政策正对应了中国宪法序言中写明的外交政策原则,即独立自主、和平发展、互利共赢,反对帝国主义、霸权主义和殖民主义。

四是全球南方模式。印度、印尼、巴西等国开始在大国夹缝中寻找数字自主空间。一些国家强调“数据主权”与“数据民族主义”,试图通过本地数据中心建设、国家平台替代、立法保护等方式实现数据本地化。另一些国家则选择与欧盟或美国主导的合作机制接轨,寻求外部投资与本国监管之间的平衡。这些国家往往成为全球数据秩序多边调和的关键变量。

全球数字秩序的演变,可类比罗马帝国及其衰落后的欧洲历史。第一阶段是“数字罗马帝国”时期(约 20 世纪 90 年代至 2015 年),美国居于秩序核心,依托互联网基础设施、开放协议与全球平台,实质掌控信息空间,构建起类似罗马普遍主义的分布式自由网络秩序,权力却集中于中心。第二阶段为“数字帝国崩解期”(2016 年至今)。自“棱镜门”“剑桥门”“通俄门”等事件暴露平台滥权与安全隐患后,各国纷纷启动再主权化,强化数据本地化与网络安全,动摇了以美国为中心的全球秩序。第三阶段正在酝酿,呈现“数据疆域化”的趋势。各国推动本地化治理,平台适应属地法规,治理模式多元并存。各类准条约机制、合规协定和主权互认机制逐步成型,类似“威斯特伐利亚前夜”格局:主权重组、规则博弈与协商体系同步建构。

传统的国家主权原则在数字时代遭遇了重大挑战。信息流动的“超主权”特性、平台的事实治理能力,以及全球互联带来的难以闭关锁国的现实,使得所谓“数字威斯特伐利亚”难以真正成形。当前全球数据治理并未陷入无序,但正处于高度竞争、低度协调的“权力空窗期”。新秩序未立,旧秩序难守,执法的即兴发挥与地缘政治的焦虑相互交织。谁能提出可持续、可扩散、具有适配性的治理框架,谁就可能在未来“数据天下”中赢得先机。

(二)数字规则的全球博弈与制度竞争

用中国传统语汇来说,当前全球数字格局呈现为制度竞争中的“合纵连横”。国家间竞争不止于表面制度差异,更体现在标准设定权与架构控制权的争夺上。大国纷纷尝试将自身数据治理规范上升为国际标准,且不再局限于条约或多边协议,而是体现在技术架构、合规体系和司法权外延等多个维度。

这种竞争表现为以下四种模式。一是欧盟的标准外溢模式。GDPR 域外适用迫使所有与欧盟用户有关的数据处理活动遵循其规则,建立起“数据合法性高地”。欧盟还通过“充分性认定机制”评估第三国数据保护体系,塑造了全球数据治理的“合规边界”。近年来,欧盟通过《数字服务法案》和《数字市场

法》扩展平台监管逻辑,进一步使欧洲规范外溢为制度力量。二是美国的平台主宰模式。美国通过《云法案》确立对全球范围内由美企控制数据的调取权力,体现出其技术基础设施嵌入全球数据流的优势。美国政府还以“国家安全”之名,强制推动对中资平台进行“所有权剥离”或“技术信任验证”,将其数字战略主张嵌入私营平台治理之中。同时,美国倡导“数据自由流动”理念,在CPTPP、IPEF、DFFT等经济合作平台中嵌入数据政策主张,试图构建一个以美式治理价值为基础的数据准则联盟。三是中国的数据安全模式。中国推动形成《全球数据安全倡议》,主张各国对数据治理应尊重国家主权,反对滥用技术手段进行数据获取与监控。通过“一带一路”合作机制,中国协助沿线国家建立本地数据中心、提供云计算基础设施,并输出配套的数据治理法律咨询方案,推动“数据基础设施本地化与合规话语本土化”的双轨机制。中国与中亚、东南亚等地区签署多边数字协议,试图从南南合作中建立具有包容性的数据治理秩序。四是“全球南方”国家的战略博弈。如印度主张“数据民族主义”,推动制定其《个人数据保护法案》,并通过封禁TikTok、要求WhatsApp本地化等手段强化主权控制力。印尼等国家则更关注数字贸易与主权并存的协调机制,参与亚太数字框架下的数据标准制定。在这些国家眼中,数据不仅是治理问题,更是经济安全与文化主权的重要资产和战略领域。

上述格局与战国时代的“合纵连横”战略极为相似。各国在“技术—法律—价值”维度上形成联盟或对抗的复合态势。平台作为国家战略的延伸,标准作为主权意志的表达,构成今日全球数据治理的核心战略工具。当前各国纷纷建立数据“朋友圈”,以图借平台制衡平台、借标准突破标准。

(三)全球秩序中的主权难题

虽然各国纷纷强调数据主权的重要性,甚至将其视为数据治理的正当性来源和合法性基础,但主权本身在数字时代面临诸多难题。

一是主权冲突化。不同国家的合法数据主张在跨境活动中常常发生直接冲突。一方面,美国以国家安全为由要求TikTok出售美国业务,或者通过《云法案》要求在外国的美企须配合提供数据;另一方面,中国《数据安全法》明确规定,境内数据需经审查批准方可出境,导致很多中国背景的企业在英美法系法院的诉讼中,面临提交境内数据难以同时满足英美法系证据开示规则和履行本国数据安全义务之间的两难。

二是主权弥散化。平台技术的全球部署削弱了传统疆域内的主权完整性。国家对数据的掌控能力愈发受限于其对基础架构的控制力,而数据治理中的强主权主张又加剧了制度间的不协调与合规冲突。如美国平台在全球范围内部署内容交付网络(CDN)和云端服务,使数据传输早已跨越了地理边界。即便欧盟制定了严格的法律规则,但若无法控制数据的流经路径与存储节点,也难以实现技术落地。印度政府虽然要求社交媒体企业“本地化”数据,但技术层面对其执行的监管权仍高度依赖美国架构。平台越全球化,国家边界对数据的控制就越困难。

三是主权错位化。全球科技平台通过技术优势与生态锁定掌握实际数据支配力,逐步演化为准主权单位。超级平台拥有用户身份识别、数据调取、行为惩戒等超越国家的权能,事实上成为“主权代理”,甚至“主权替代”。在某些时刻,超级平台甚至能够影响到战争:“对世界上最大的一些科技公司而言,俄乌冲突已经成为一个决定性的地缘政治时刻。它们的平台已经成为一场平行信息战的主战场,数据和服务成为冲突中的关键环节。”①

三类悖论使数据主权在现实操作中无法像传统主权那样封闭自洽,而转向动态嵌套、冲突协商的新型治理模式。主权既是国家抵御外部操控的合法依据,也是构建国际主导权的竞争手段。数据主权成为全球数字治理的基础“矛盾”:既是保护之盾,也是扩张之矛。

---

① Adam Satariano & Sheera Frenkel, *Ukraine War Tests the Power of Tech Giants*, New York Times, March 1, 2022.

结　语

在全球数据治理的语境中,主权未亡,形态已变;规则未定,天下未一。世界既难回归“数字威斯特伐利亚”式的主权分立,也难以达成“大一统”的集中治理。更现实的图景,是以主权国家为基本单元、区域机制为中介、国际组织和跨国平台有限协作为补充的多中心治理格局。在“数字战国”格局中,核心问题不再是由谁统一“数字天下”,而是未来的数据秩序由谁设计、执行、监督与共享。国家、平台与制度机制之间正围绕数据主权展开制度创新与法律嵌套的多维博弈,主权从传统控制逐渐转向对数据流通、安全与规则制定权的主张。这种弹性的主权观反映了现代主权内涵的转型:从领土型向关系型、从排他性向协同性、从静态边界向动态网络演化。唯有在此张力中准确定位国家角色,正视价值正当性、制度建构与技术能力的交织互动,方能为全球数字秩序奠定更为稳固与包容的治理基础。

The Concept of Data Sovereignty: Resilient Sovereignty in Global Digital Geopolitics

Liu Han

(*School of Law*, *Tsinghua University*, *Beijing* 100084, *China*)

Abstract: Against the backdrop of profound transformations in the global digital order, “data sovereignty” has increasingly emerged as a key discursive instrument through which states reaffirm national control, address the imbalance of platform governance, and regulate cross-border data flows. Data sovereignty should not be conceived as a mere digital extension of traditional territorial sovereignty, but rather as a flexible and elastic form of sovereignty that simultaneously embodies both expansionary and defensive characteristics. Theoretically, two distinct types of data sovereignty can be identified: “negative data sovereignty”—manifested in data localization, defensive measures, and territorial control—and “positive data sovereignty”—expressed through regulatory externalization, platform embedding, and infrastructural dominance. The dynamic interplay between these two forms of sovereignty has generated new tensions among sovereign states, digital platforms, and transnational legal regimes. From the perspective of global digital governance, it is necessary to reconstruct the legitimacy and normative foundations of the emerging data order on the basis of a new theory of sovereignty that transcends traditional territorial paradigms.

Key words: data sovereignty; cross-border data flow; positive sovereignty; negative sovereignty; global governance

(责任编辑　郭昌盛)